PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-016255
(43)Date of publication of application : 19.01.2001

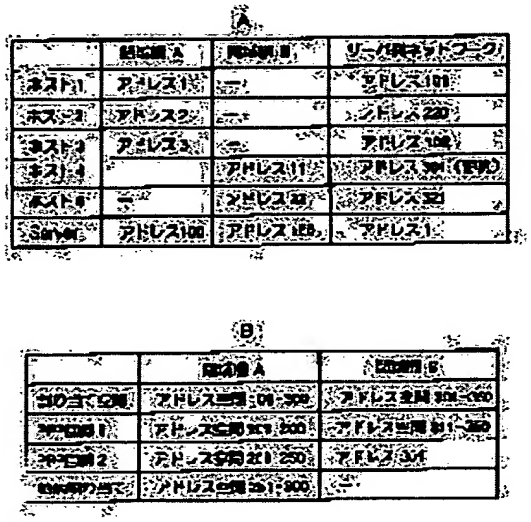
(51)Int.Cl. H04L 12/56
H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 11-183067
(22)Date of filing : 29.06.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : TERAO KAZUYUKI
ONO SATOSHI

(54) INTER-NETWORK COMMUNICATION METHOD AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To operate physically one server as if each closed area network had a server in the communication between a plurality of the closed area networks and a server side network.
SOLUTION: In this communication method, when an access server AS has a point-to-point protocol PPP connection request from a terminal in a closed area network to a server, which PPP line in which closed area network is identified, a corresponding line is selected in an address space (Figure B) at a server side assigned in advance by PPP lines of closed area networks, an address of a terminal of the closed area network is made to correspond to the selected line (Figure A), address conversion is applied to a packet and the packet is sent to the server side network. The packet from the server side network is address converted by referring to the Figure A, which PPP line in which closed area network is recognized and the packet is sent to the line.



LEGAL STATUS

[Date of request for examination]	29.06.1999
[Date of sending the examiner's decision of rejection]	15.10.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3394727
[Date of registration]	31.01.2003
[Number of appeal against examiner's decision of rejection]	2002-21936
[Date of requesting appeal against examiner's decision of rejection]	13.11.2002
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－16255
（P2001－16255A）
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	
12/66				

審査請求　有　請求項の数13　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－183067

(22)出願日　平成11年６月29日(1999.6.29)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　寺尾　和幸
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

Ｆターム(参考)　5K030 GA15 HD08 HD09 KA01 KA04
5K033 BA04 CB09 CC01 DA06 DB12

(54)【発明の名称】　ネットワーク間通信方法及びその装置

(57)【要約】
【課題】　複数閉域網とサーバ側ネットワークとの間の通信で、物理的に１台のサーバを各閉域網にそれぞれサーバがあるかのように動作させる。
【解決手段】　閉域網の端末からサーバへのＰＰＰ接続要求がアクセスサーバＡＳにあると、どの閉域網のどのＰＰＰ回線であるかを識別し、閉域網のＰＰＰ回線ごとに予め割り当てたサーバ側のアドレス空間（図２Ｂ）の中から対応する１つを選択して、その閉域網の端末のアドレスを対応付け（図２Ａ）、パケットをこのアドレス変換を行ってサーバ側ネットワークへ送る。サーバ側ネットワークからのパケットを、図２Ａを参照してアドレス変換すると共に、どの閉域網のどのＰＰＰ回線かを知り、その回線にパケットを送る。

A

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト１	アドレス１	－	アドレス 101
ホスト２	アドレス２	－	アドレス 220
ホスト３	アドレス３	－	アドレス 102
ホスト４	－	アドレス 11	アドレス 301（静的）
ホスト５	－	アドレス 22	アドレス 321
Server	アドレス100	アドレス 150	アドレス１

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間 101-300	アドレス空間 301-350
PPP回線１	アドレス空間 101-200	アドレス空間 311-350
PPP回線２	アドレス空間 201-250	アドレス 301
動的割り当て	アドレス空間 251-300	－

図２

1

【特許請求の範囲】

【請求項１】　複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol)を利用して接続して通信を行う方法において、
ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
サーバ側ネットワークで、予め各ユーザ側ネットワークごとにそれぞれ割り当てた複数のアドレス空間における、上記認証したネットワーク及びＰＰＰ回線に対するアドレス空間から選んだアドレスに、そのユーザ側ネットワークのＰＰＰ回線からのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送り、
かつその変換アドレスと変換前のアドレスと、認証したユーザ側ネットワーク及びＰＰＰ回線との対応表を記憶しておき、
サーバ側ネットワークからのパケットのアドレスを上記対応表を参照して上記アドレス変換の逆変換を行って対応するユーザ側ネットワークのＰＰＰ回線へ送ることを特徴とするネットワーク間通信方法。

【請求項２】　上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのデスティネーションアドレスをサーバ側ネットワークにおける該当するアドレスに変換することを特徴とする請求項１記載のネットワーク間通信方法。

【請求項３】　上記アドレス変換の際に、上記ユーザ側ネットワークからのパケットのサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換することを特徴とする請求項１又は２記載のネットワーク間通信方法。

【請求項４】　上記アドレスの選択はユーザ側ネットワークの利用方針に応じて動的又は静的に行うことを特徴とする請求項１乃至３の何れかに記載のネットワーク間通信方法。

【請求項５】　上記ＰＰＰ接続が確立した後にそのＰＰＰ回線からのパケットは、そのアドレスにて上記対応表を参照してアドレス変換して、サーバ側ネットワークへ送信することを特徴とする請求項１乃至４の何れかに記載のネットワーク間通信方法。

【請求項６】　複数のユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol)を利用して接続して通信を行う方法において、
ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
予め各ユーザ側ネットワークのＰＰＰ回線毎に割り当てたＶＬＡＮ（VirtualＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報を、上記認証されたユーザ側ネットワークのＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送り、
サーバ側ネットワークからのパケットのＶＬＡＮを識別する情報から求めたユーザ側ネットワークのＰＰＰ回線

2

にそのパケットを送ることを特徴とするネットワーク間通信方法。

【請求項７】　複数ユーザ側ネットワークのそれぞれとサーバ側ネットワークとをＰＰＰ（Point-to-Point Protocol)を利用して接続して通信を行う方法において、
ＰＰＰ接続確立時に、そのＰＰＰ回線が所属するユーザ側ネットワークを認証し、
予め各ユーザ側ネットワークごとに割り当てたＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報を、上記認証されたユーザ側ネットワークのＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送り、
かつそのパケットのアドレスとＶＬＡＮを識別する情報とＰＰＰ回線との対応表を記憶しておき、
サーバ側ネットワークからのパケットのＶＬＡＮを識別する情報及びアドレスから上記対応表を参照してＰＰＰ回線を求めて、そのパケットをユーザ側ネットワークのそのＰＰＰ回線に送ることを特徴とするネットワーク間通信方法。

【請求項８】　複数のユーザ側ネットワークとＰＰＰ（Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、
各ユーザ側ネットワークのＰＰＰ回線ごとに割り当てられたアドレス空間を記憶するアドレス空間割り当てテーブルと、
接続してくる端末がどのユーザ側ネットワークのどのＰＰＰ回線に属するかの認証を行う手段と、
上記認証されたユーザ側ネットワークのＰＰＰ回線に対し、上記アドレス空間割り当てテーブルで割り当てられている１つのアドレスに、上記ＰＰＰ回線よりのパケットのアドレスを変換してそのパケットをサーバ側ネットワークへ送るアドレス変換手段と、
上記アドレス変換されたアドレスと変換前のアドレスとの関係を記憶する変換アドレス記憶手段と、
サーバ側ネットワークからのパケットのアドレスを上記変換アドレス記憶手段を参照して変換し、かつ上記テーブルを参照して対応するユーザ側ネットワークのＰＰＰ回線へそのパケットを送るアドレス逆変換手段とを具備するアクセスサーバ装置。

【請求項９】　ユーザ側ネットワークのＰＰＰ回線からのパケットを、そのアドレスにより上記変換アドレス記憶手段を参照してアドレス変換してサーバ側ネットワークへ送る手段を備えることを特徴とする請求項８記載のアクセスサーバ装置。

【請求項１０】　上記アドレス変換手段はパケットのデスティネーションアドレスをサーバ側ネットワークの該当するアドレスに変換する手段を備えることを特徴とする請求項８又は９記載のアクセスサーバ装置。

【請求項１１】　上記アドレス変換手段は、パケット中

のサーバに対するポート番号を、そのユーザ側ネットワークに固有のポート番号に変換する手段も備えることを特徴とする請求項８乃至１０の何れかに記載のアクセスサーバ装置。

【請求項１２】　複数のユーザ側ネットワークとＰＰＰ（Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークのＰＰＰ回線とＶＬＡＮ（Virtua１ ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報との関係を記憶したＶＬＡＮ識別情報テーブルと、

ＰＰＰ接続確立時に、そのＰＰＰ回線がどのユーザ側ネットワークに属するかの認証を行う手段と、

上記認証されたユーザ側ネットワークのＰＰＰ回線と対応するＶＬＡＮを識別する情報を、上記テーブルを参照して求め、上記ＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

サーバ側ネットワークよりのパケットを、そのＶＬＡＮを識別する情報から上記テーブルを参照して対応するユーザ側ネットワークのＰＰＰ回線へ送る手段とを具備するアクセスサーバ装置。

【請求項１３】　複数のユーザ側ネットワークとＰＰＰ（Point-to-Point Protocol)により接続されるサーバ側ネットワークとの間に設けられるアクセスサーバ装置であって、

ユーザ側ネットワークとＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報との関係を記憶したＶＬＡＮ識別情報テーブルと、

ＰＰＰ接続確立時に、そのＰＰＰ回線がどのユーザ側ネットワークに属するかを認証する手段と、

上記認証されたユーザ側ネットと対応するＶＬＡＮを識別する情報を上記テーブルを参照して求め、上記ＰＰＰ回線よりのパケットに付加してサーバ側ネットワークへ送る手段と、

上記パケットのアドレスと、上記ＶＬＡＮを識別する情報と上記ＰＰＰ回線との対応表を記憶する手段と、

サーバ側ネットワークよりのパケットを、そのＶＬＡＮを識別する情報とアドレスとから、上記テーブル及び上記対応表を参照して対応するユーザ側ネットワークのＰＰＰ回線へ送る手段とを具備するアクセスサーバ装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は異なる複数のネットワーク、特に閉域網間の通信を行うエクストラネット向けの共有サーバのホスティングサービス（各ユーザ側ネットワークに貸出すサービス）の提供や、チケット予約サービスなどパブリックなサービスをこれらのユーザ側ネットワーク（閉域網）上のサーバの持つ情報を組み込むことによりユーザ側ネットワーク（閉域網）単位でカスタマイズした（各ユーザ側ネットワークのニーズに応じた）サービスを安全に提供するなど電子商取り引きを含めた情報流通通信方法及びその装置に関する。

【０００２】

【従来の技術】今日インターネットを始めネットワークの利用は広く普及し、多くの企業においては企業内の通信費用を安く抑えかつ、安全に行うために閉域網の構築を行っている。この構築においては、専用線だけでなくＡＴＭ、ＦＲ（フレームリレー）を用いたり、ＩＰ（インターネットプロトコル）トンネリングを利用して行っている。また、営業マンなどが外出先からこれらの閉域網に接続する場合には、ＰＰＰ（Point-to-Point Protocol)やその拡張であるＬ２ＴＰ（Layer2 tunneling Protocol)を用いている。閉域網間の通信が今後増加し、複数の閉域網で利用する共用サーバを自閉域網の閉域性を失うことなく提供したり、チケット予約サービスなどのパブリックなサービスを、各閉域網上のサーバの持つ情報と組み合わせてカスタマイズしての利用が増える。これの実現方法として、各閉域網上にサービスを提供するサーバを用意する方法があるがこれはコストがかかり、サーバを用意する側の負担が大きい。そこで、物理的には１台のサーバであるが、各閉域網からは各々別々のサーバが存在するように見え、カスタマイズしたサービスをセキュア（安全）に提供できる仮想プライベートサーバの構築を考える。

【０００３】現在、企業などの閉域網の構築においては、ネットワークの急激な普及によるＩＰアドレスの不足のために、ローカルアドレスを用いるか、インターネットなど外部に接続する時にのみ動的にグローバルアドレスを付与して外部と通信を行う方法が取られている。しかし、動的にアドレスを付与する場合、次回の接続時には同一のアドレスを付与されるとは限らないので、特に移動端末など必要時にしか接続しない／その接続自体が不安定である場合、静的にアドレスを付与することがより必要となる。また、動的にアドレスを付与する状況ではサーバ側から特定の端末への接続確立は困難であるので、ネットワーク構築時にローカルアドレスを静的に付与する場合が多い。物理的に１台のサーバでこのように構築されている閉域網に対してのサービス提供を考えた場合、（１）サーバ側ネットワークを介した不正な接続など防止、（２）接続している閉域網間におけるアドレス空間の衝突、（３）サーバから移動端末を含めた特定の端末への接続確立、という３つの問題の解決が必要となる。

【０００４】このサーバの構築には、既存技術のＬ２ＴＰ（Layer2 tunneling Protocol)に代表されるＰＰＰトンネリング技術、ＮＡＴ（Network Address Translator）に代表されるアドレス変換技術の２種類が有用な技術であるといえる。まず、ＰＰＰトンネリング技術により移動端末は時間と場所に制約されずに常に自分の閉域網への接続が可能になり、あたかもその閉域網に存在し

ているかのように閉域網の利用が可能になる。また、図２２に示すように閉域網Ａ，Ｂがインターネット／公衆網を介してサーバ側ネットワークと接続可とされ、各閉域網Ａ，Ｂに属するホスト（端末とも云う）にはそれぞれのローカルアドレス空間Ａ，Ｂでのアドレスが与えられており、各ホストはそれが属する閉域網の網間アクセスサーバ（ＡＳ）を通じ、ＰＰＰトンネリングを利用してサーバ側ネットワークの網間アクセスサーバと接続してサーバと接続可能とされている。この構成により、ＰＰＰ接続をサーバ側までトンネリングすることで端末に、あたかも自分の閉域網に属するサーバと接続しているように見せることができる。これにより、閉域網の持つ閉域性を維持したり、閉域網で割り当てられているローカルアドレスをそのまま使用することが可能になる。しかし、

（１）閉域網では端末にローカルアドレスを自由に割り当てるので、複数の異なる閉域網に属する端末が同一のアドレスを持つ場合が生じ、この場合は衝突が避けられない。そのため、接続先のサーバ側ネットワークから見ると同一のアドレスを持つ端末が複数存在することが発生し、この時どの端末と通信しているかを正しく認識することが出来ない。

【０００５】（２）サーバを示すアドレスを各閉域網で共通にする必要があり既存の設備への大幅な変更が必要になる場合がある。

（３）端末からの接続確立時にサーバ側からアドレスを動的に割り当てる場合、移動端末のように必要に応じてネットワークに接続してくる端末にはどのアドレスが割り当てられているか不明であって、有用なサービスであるサーバ側からの情報配信といったサービスの提供が不可能である、

（４）サーバ側のネットワークを介して、閉域側をまたぐ不正アクセス発生の可能性がある、といった問題があり、すべての課題の解決ができない。

【０００６】また、閉域網に接続しているローカルアドレスを付与されたユーザ端末がインターネット上のグローバルアドレスを付与されたサーバとの通信を行うには、ユーザ端末自身もグローバルなアドレスを持つ必要がある。しかし、前述のようにグローバルアドレスは不足するため端末にはローカルアドレスを静的に割り当てている場合が多い。この時ＮＡＴ（ネットワークアドレス変換）技術により、図２３に示すように閉域網内の通信はローカルアドレスを用いて行い、インターネット上のWWWサーバとの通信には、網間境界に設けたＮＡＴを利用できる装置にあらかじめプールされたグローバルなアドレスを動的に割り当てて通信を可能にする。しかし、このＮＡＴは動的にローカルアドレスとグローバルアドレスと対応つける／アドレスとポート番号の組によりホスト（端末）間の接続の識別を行うために、（１）ホストとサーバ間の接続は動的に認識されるので、一旦接続が切断した後のローカルアドレスを静的に割り当てた端末へのグローバルアドレスを持つサーバ側からの情報配信などのプッシュ型（端末からの接続確立要求なし）のサービスは不可能、（２）サーバが各閉域網ごとの認証（識別）を行うことができないため、各所属端末毎にカスタマイズしたサービスや情報を提供することが困難、（３）ＮＡＴの部分はグローバルなアドレス空間に接続しているので不正アクセスの可能性、といった問題があり、サーバ構築におけるすべての問題の解決ができない。

【０００７】また、ＮＡＴ技術自体は様々な形で拡張・利用されており、この明細書で課題としているサーバの構築に利用可能と考えられるものに、ＰＰＰと連携したＮＡＴ技術や、設定によりパケットのソースアドレスとデスティネーションアドレスの双方の変換を行えるＣｉｓｃｏ社によるＮＡＴ技術がある。ＰＰＰと連携したＮＡＴにおいては、サーバとの間にＰＰＰ接続を確立後、サーバよりふり出されたグローバルＩＰアドレスを用いて、ＰＰＰ回線を経由して外部のインターネットなどのグローバルＩＰネットワークとの通信においてＮＡＴ機能を行うものである。つまり確立されたＰＰＰ回線単位のＮＡＴが可能になっている。この技術を利用して課題のサーバの構築を考える。この技術をサーバ側の装置に導入すると、ＰＰＰ回線毎にＮＡＴを行えるので閉域網単位で利用するサービスをカスタマイズしたり、利用するサーバを各閉域網単位で変更することが容易にできる。しかし、１台のサーバによる実現を考えると、次の問題がある。

【０００８】

【発明が解決しようとする課題】（１）クライアントに相当するユーザの閉域網とサーバ側のネットワークがＰＰＰ接続により接続されるのでＰＰＰトンネリング技術を利用する場合と同様に、ローカルアドレスで構築された閉域網同士の接続においてはアドレス空間の衝突が生じることになる。特に、この技術をサーバ側に導入するとクライアントに相当する閉域網のホストから到着したパケットを受けとったサーバが、閉域網のホストを示すアドレス部分の重複によりそのパケットがどの閉域網のホストから来たのかが識別できず、正しく該当するホストへパケットを送り出すことができない。

【０００９】（２）ＰＰＰ接続確立時にふりだされたアドレスに対してＮＡＴを行うので、そのアドレスに対してサーバ側の複数のサーバの持つアドレスがマッピングされるので、ユーザの閉域網のホストから複数あるサーバのうち特定のサーバへの接続を確立することができない。確立するには、利用したいサーバの数に応じてＰＰＰ回線を確立し、ＰＰＰにより取り決められるアドレスに対してサーバのアドレスを一つ対応させることが必要になる。

【００１０】（３）サーバを示すアドレスに対して変換

7

を行うのだが、変換後のアドレスが閉域網のホストを示すアドレスと同一になると正しく通信が行えない。そのため、各閉域網のホストの利用するアドレスとサーバ側ネットワークのサーバのアドレスとが重ならないようにする必要があり、各閉域網でどのようなローカルアドレスを用いるかを調べて、サーバ側ネットワークのアドレスを決めるため多大な手間と時間がかかる。

【００１１】といった問題があり解決できない、Ｃｉｓｃｏ社の開発したＮＡＴ技術は、ＲＦＣ１６３１で定義されているＮＡＴとは異なり、対象となるパケットのソースアドレスとデスティネーションアドレスの双方に対してアドレスの静的／動的な割り当てによるアドレス変換表を用いてアドレス変換が可能であり、アプリケーション層との連携、特にＤＮＳ（Domain Name System）との連携によるＮＡＴに利用するアドレス変換表を作成しての柔軟な動作が可能である。このような特徴により、従来のＮＡＴ技術では難しかったグローバルアドレスを持つインターネット上のサーバなどからＮＡＴ装置の後ろに接続されているローカルアドレスで構築された閉域網上のホストへの接続確立をも可能にしている。また、受けとったパケットの外部のホストを示すアドレスがアドレス変換表にない場合はパケットを破棄したり、または、外部のネットワークに通知するアドレスを制限するなどにより閉域網の持つ閉域性を保つこともできる。この技術を用いてこの明細書で考えるサーバの構築を行うと、（１）サーバ側ネットワークもローカルアドレスで構築された閉域網の場合、アドレス空間の衝突を避け、インターネット上のサーバなど閉域網の外のホストと通信するために双方のネットワークでＮＡＴを行う。この時、閉域網間で通信を行うにはＮＡＴに利用するグローバルアドレスとホストの持つローカルアドレスを少なくとも１対１対応にしない限り接続先のホストを特定できないため通信ができずに駄目である。この場合サーバ側から閉域網のホストへの接続ができないだけでなく、複数のサーバが存在する場合には、前述の理由により特定のサーバへの接続もできない。

【００１２】といった問題がありすべてを解決できない。このように、既存の技術を用いた場合この明細書で述べているサーバ構築に生じる問題の全てを解決し得ない。

【００１３】

【課題を解決するための手段】第１発明

第１発明、第２発明においてもユーザの利用している複数のユーザ側ネットワーク（以後、ユーザ側ネットワークを閉域網として説明する）はサーバ側のネットワークにＰＰＰ（Point-to-Point Protocol)による接続を行う。このＰＰＰ接続確立時の認証において従来のユーザの認証に加え、ＰＰＰ接続を行ってきた接続元がどの閉域網のどのＰＰＰ回線かの認証を行う。第１発明によればその結果により、接続しているＰＰＰ接続がどの閉域

8

網のどのＰＰＰ回線かを示す情報を各ＰＰＰ回線に対応付ける。そして、この情報をキーとして該当するＰＰＰ回線に割り当てられたサーバ側ネットワークのアドレスと、必要に応じて閉域網単位に決められた利用するサーバのサービスに応じたポート番号を用いて、ＰＰＰ回線を通してサーバ側ネットワークに入ってくる／から出ていくパケットに対してソースとデスティネーションの両方のネットワークアドレスと必要に応じてポート番号の変換を行う。

【００１４】この第１発明では、サーバ側ネットワークにおいて各閉域網単位にアドレス空間を独自に割り当て、その閉域網単位の方針による柔軟な利用を行う。サーバ側ネットワークにおいて各閉域網に用意されたアドレス空間は、次の方針により割り当てる。まずＰＰＰ回線単位に静的にアドレス空間を割り当てる。このアドレス空間は、サブネット単位で割り当てることにする。静的な割り当て分がなくてもよい。その場合は、全て動的にサブネット単位でＰＰＰ回線に割り当てる。そして、もし残った空間があれば割り当てられたアドレス空間を消費してしまったＰＰＰ回線に対して、ＰＰＰのＬＣＰ（設定プロトコル）などを用いて動的にＰＰＰ回線に割り当てるものとする。動的に割り当てるアドレス空間の大きさは、動的にネゴシエーションにより必要分でもよいし、一定の大きさを決めておいてもよいし、あるアルゴリズムにより徐々に大きさを大きくするなど自由に選択できる。また、動的にＰＰＰ回線を割り当てた場合、どのアドレス空間をその閉域網のどのＰＰＰ回線に割り当てたかを管理しておくことで、サーバ側から閉域網側の端末へのパケットを適切なＰＰＰ回線に送り出すことができる。

【００１５】このように閉域網単位で割り当てを含め動作が独立しているので、接続してくる閉域網のアドレス空間の衝突による問題の回避や、特定端末への接続を可能にしている。また、アドレスの変換はサーバ側で行われており、サーバ側で接続に関する制御が容易にでき、各閉域網の持つ閉域性を維持できるだけでなく、接続する閉域網側で、自閉域網のアドレス空間から自由に利用するサーバにアドレスを付与することが可能であり、導入時に伴うネットワークの設定変更は最小限に抑えることができる。以下、このアドレス変換方法を、ルートサイドＮＡＴ（以下、Root-side ＮＡＴもしくはＲＮＡＴ）と呼ぶ。

第２発明

第１発明と同様にＰＰＰ接続確立時にその回線の属するユーザの閉域網がどれかの認証を行う。そして、ＰＰＰ接続確立時の所属の閉域網の認証を終了後に、ＰＰＰ回線にそれがどの閉域網のどのＰＰＰ回線かを識別できるに十分なＶＬＡＮ（Virtual ＬＡＮ）を利用する時に利用するＶＬＡＮを識別する情報とを対応付ける。そして、このＶＬＡＮを識別する情報をもとにスイッチング

などのＶＬＡＮ構成技術により、利用するサーバへそのＰＰＰ回線よりのパケットを運ぶ。そして、１台のサーバにおいて各ＶＬＡＮを識別する情報単位に各種処理を行うＯＳを動作させ前述のサーバを実現する。

【００１６】また、ＰＰＰ回線に閉域網を識別するに十分なＶＬＡＮを識別する情報を対応付ける場合は、パケットを受けとったＰＰＰ回線とそのパケットに示された閉域網のホストのアドレスを対応付ける。なお、この対応付けは、ＶＬＡＮを識別する情報単位に行う。これにより、ユーザのネットワークに変更を加えることなく、ＶＬＡＮを識別する情報を利用したサーバ側ネットワークの制御により容易に上述のサーバを構築、利用できる。この所属する閉域網に関する認証結果により、確立されたＰＰＰ回線に少なくとも閉域網を識別できるＶＬＡＮを識別する情報を割り当てる方法を以下、ＶＮＡＴと呼ぶ。

【００１７】

【発明の実施の形態】第１発明

まず第１発明について実施の形態を説明する。いま図１に示すシステム構成とされているとする。即ち、閉域網Ａ，Ｂ，Ｃがインターネット／公衆網とそれぞれアクセスサーバＡＳを介して接続され、インターネット／公衆網とサーバ側ネットワークが、この発明によるRoot-side ＮＡＴ機能付きアクセスサーバＲ－ＮＡＴを介して接続されている。閉域網Ａ，Ｂにおいて各ホスト（端末）に対して図２Ａに示すようにアドレスが割り当てられている。つまり閉域網Ａの持つアドレス空間において、ホスト１にはアドレス１、ホスト２にはアドレス２、ホスト３にはアドレス３、利用するServerにはアドレス１００が割り当てられているとする。Serverはサーバ側のネットワークにおかれているホストの一つであり、このServerはサーバ側のネットワークにおいて、アドレス１が与えられている。さらに、サーバ側のネットワークにおいては図２Ｂに示すように閉域網Ａ，Ｂに対してそれぞれ固有のアドレス空間が用意されている。閉域網Ａから接続してくる端末用にアドレス群１０１～３００を用意しており、そのうち、ホスト１とホスト３の利用しているＰＰＰ回線１から接続してくる端末用にアドレス群１０１～２００を、ホスト２が利用しているＰＰＰ回線２から接続してくる端末用にアドレス群２０１～２５０をそれぞれ割り当てている。そして、残りのアドレス群２５１～３００は、前述の割り当てを使い切った場合に、ＰＰＰ回線１，２に対して動的に必要に応じて割り当てる。閉域網Ｂの持つアドレス空間において、ホスト４にはアドレス１１、ホスト５にはアドレス２２、利用するServerにはアドレス１５０が各々割り当てられている。さらに、サーバ側のネットワークにおいては閉域網Ｂから接続してくる端末用にアドレス群３０１～３５０を用意しており、そのうち、アドレス群３０１～３１０までは閉域網Ｂの端末が直接確立するＰＰＰ回線に静的に割り当てられている。また、３１１～３５０まではＰＰＰ回線１に割り当てられており、このＰＰＰ回線を利用してくるホストにサーバ接続時に動的に割り当てるものとする。このように、サーバ側のネットワークで各閉域網単位にアドレス空間をプールし、アドレス空間を閉域網の利用方針に応じてＰＰＰ回線に割り当て、そこから更に該当するＰＰＰ回線を利用するホストへ静的、動的を含め柔軟に割り振る。

【００１８】また、各閉域網におかれたアクセスサーバＡＳとRoot-side ＮＡＴの機能を持つ装置Ｒ－ＮＡＴとの間はＰＰＰ接続されている。また、閉域網の端末は、このＰＰＰ接続を利用してサーバを利用するか、ＰＰＰトンネリングを利用して直接サーバ側におかれたRoot-side ＮＡＴ機能付き装置（Ｒ－ＮＡＴ）とＰＰＰ接続を行いサーバを利用する。

【００１９】そこで、サーバ側のネットワーク上の物理的に１台のサーバを各閉域網にあたかも各々存在するように仮想的に見せ、各閉域網の閉域性を失うことなく複数閉域網において利用可能にするのが、このRoot-side ＮＡＴである。このRoot-side ＮＡＴはサーバ側で各閉域網毎に、あらかじめ用意したアドレスを割り当てるに際し、閉域網とのＰＰＰ接続確立時に接続を要求している端末が正しいかどうかというホストに関する従来の認証だけでなく、接続してくる端末がどの閉域網のどのＰＰＰ回線に属するかの認証を行う。この結果を基に、あらかじめその閉域網のＰＰＰ回線に用意されたアドレス群の中から端末に静的にアドレスが割り振られている場合は該当するものを、そうでない場合は、ＰＰＰ回線単位に用意されたアドレス空間から端末に動的にアドレスを割り振る。

【００２０】図１において、ホスト１が接続してきた時、ＰＰＰ回線がまだ確立していない場合、利用しているＡＳ（アクセスサーバ）からＰＰＰ回線の確立がはじまり、この時、このＰＰＰ回線が閉域網ＡからのＰＰＰ回線１であることの認証を行う。そして、この閉域網ＡのＰＰＰ回線１用にプールされたアドレス空間からアドレスをホストに対して動的に割り当てる。今回の場合、ＰＰＰ回線１には、図２Ｂに示すようにアドレス空間１０１－２００が与えられており、この空間から動的に与えるので、ホスト１には、利用されていないアドレス１０１をサーバ側ネットワークにおいて割り当てる。つまり、ＲＮＡＴにより閉域網ＡのＰＰＰ回線１よりのパケットについて閉域網Ａで与えられているアドレス１がアドレス１０１に変換されることになる。この関係が図２Ａに示すように表として記憶される。その後、閉域網ＡのＰＰＰ回線１を通してホスト１からパケットが到来すると、そのアドレス１により図２Ａの表を参照してサーバ側ネットワークのアドレス１０１に変換される。同様に、ホスト３からのパケットが来た場合は、ＰＰＰ回線１からということで同一のアドレス空間から動的にホス

ト３に、利用されていないアドレス１０２が割り当てられ、ＲＮＡＴによりホスト３の持つアドレス３がアドレス１０２に変換される。ホスト２がサーバに接続する場合、別のＰＰＰ回線であるＰＰＰ回線２を利用しているので、ＰＰＰ回線２用に用意されたアドレス空間２０１－２５０から割り当てることになり、利用されていないアドレス２２０がサーバ側のネットワークで割り当てられ、ＲＮＡＴによりアドレス２がアドレス２２０に変換される。

【００２１】ホスト４は、ＰＰＰトンネリングを利用してサーバ側の装置に直接ＰＰＰ接続してきており、ＰＰＰ回線の確立がはじまり、この時、同様の認証によりこのＰＰＰ回線が閉域網Ｂからの ＰＰＰ回線２であることが認証される。そして、この閉域網ＢのＰＰＰ回線２には静的にアドレス３０１が割り当てられているので、ＲＮＡＴによりホスト４の持つアドレス１１がアドレス３０１にサーバ側ネットワークにおいて変換されることになる。ホスト５がサーバに接続する場合、利用するＰＰＰ回線が閉域網ＢのＰＰＰ回線１であることが認証され、ＰＰＰ回線１に用意されたアドレス空間３１１－３５０から利用されていないアドレスが動的にホスト５に割り当てられる。今回は、アドレス３１１が割り当てられている。ホスト５からサーバへのパケットは、ＲＮＡＴによりホスト５の持つアドレス２２に対してアドレス３１１へと変換される。

【００２２】また、接続先に指定されたServerのアドレスもサーバ側のネットワークにおいてServerに割り当てたアドレスへの変換を行う。今回、閉域網Ａに関してはServerのアドレス１００がアドレス１に、閉域網Ｂに関してはServerのアドレス１５０がアドレス１に変換されることになる。閉域網単位に割り当てたアドレスを基にした利用するサービスの制限も可能であるが、閉域網単位に利用するサーバのポート番号を決めておくことで、サーバのポート番号により、物理的に１台のサーバにより閉域網単位のサービス提供を可能にする。今回、Serverにおいて閉域網Ａ向けのサービスは、ポート番号Ａで、閉域網Ｂ向けのサービスは、ポート番号Ｂで提供されているとする。

【００２３】Root-side ＮＡＴは、このアドレスの対応付けとポート番号を基にパケットのソースとデスティネーション両方のネットワークアドレスとポート番号の変換とをサーバ側の管理のもとで行う。実際、ホスト１がServerのWWW Server （ポート番号８０）を利用する場合、ホスト１のパケットはＲＮＡＴにより図３に示すような変換動作が行われることになる。図３Ａはホスト１からサーバへのパケット、図３Ｂはサーバからホスト１へのパケットの各Ｒ－ＮＡＴでの変換を示す。

【００２４】つまり、Root-side ＮＡＴにおけるアドレス変換部分をまとめると、図４に示すようになる。この図においてＮｅｔＡは、サーバ側のネットワークのアドレス空間においてServerが存在しているネットワークのアドレス群、ＮｅｔＢはサーバ側のネットワークのアドレス空間における各閉域網用に用意されたアドレス群をまとめたものである。また、図５に示すように各閉域網用に用意されたアドレス群は、端末あるいは、ネットワークに接続している各ＰＰＰ回線に静的に割り当てられ、残りの空間は、静的に割り当てられている空間が足らなくなった場合に、不足しているＰＰＰ回線に対して要求に応じて動的に割り当てるために用いる。動的に割り当てられた空間は、割り当て時にどのＰＰＰ回線に割り当てたかを管理することで、パケットを適切なＰＰＰ回線に送出することができる。このように、サーバ側ネットワークに用意された空間は、各空間の利用者である閉域網が利用の方針を選択できる。各閉域網における端末のアドレスをサーバ側において閉域網毎にあらかじめ用意されたアドレスに各々対応付けることをコンパクション（Compaction）変換、各閉域網において割り振られたServerのアドレスをサーバ側のネットワークにおけるサーバのアドレスに変換することをマージ（Merge)変換と呼ぶことにする。また、逆Compaction変換は端末に割り振られたアドレスからどの閉域網のどのＰＰＰ回線かを図２Ａ，Ｂを参照して識別し、その閉域網における端末のアドレスに変換する。逆Merge 変換は逆Compaction変換から得られるどの閉域網に属する端末かの情報から、サーバのアドレスを閉域網におけるサーバのアドレスに図２Ａを参照して変換する。そして、どの閉域網のどのＰＰＰ回線かの識別により適切な閉域網の適切なＰＰＰ回線へとパケットを送り出す。この時、端末からサーバへのパケット、サーバから端末へのパケットのソースとデスティネーションアドレスに上記の変換を図６に示すように行う。また、利用しているサーバのポート番号にも関してサーバ側ネットワークにおいて閉域網単位に決めたポート番号から、閉域網において利用されているポート番号へと変換する。

【００２５】この各閉域網毎に与えられたアドレス空間は、所属する閉域網に関する認証の結果割り当てることから、各アドレスがどの閉域網であるかは認証されているので、この異なる閉域網のアドレス間の接続をサーバ側で禁止することで、結果として閉域網間の通信を禁止し、閉域網の持つ閉域性を確保できることになる。さらに、各閉域網に割り当てられたこのアドレス空間を基にしたり、各閉域網に対してサーバにおいて利用できるポート番号を決めることで提供するサービスを閉域網毎にカスタマイズすることが可能になる。従来技術と第１発明（ルートサイドＮＡＴ）の特徴を図７にまとめて示す。

第２発明

第２発明が適用されるシステム構成を図８に示す。閉域網Ａ，Ｂがそれぞれアクセスサーバ５を介してインターネット／公衆網と接続され、またサーバ側ネットワー

クがＶＮＡＴ機能付きアクセスサーバＶＮＡＴを介してインターネット／公衆網と接続されている。ＶＮＡＴ機能付きアクセスサーバＶＮＡＴでは図９に示すようにＶＬＡＮタグを各閉域網の各ＰＰＰ回線に割り当てる。以下、この割り当てによる変更をＶＮＡＴと呼ぶ。各閉域網におかれたアクセスサーバＡＳは、サーバ側ネットワークにあるＶＮＡＴ機能を持つアクセスサーバＶＮＡＴにＰＰＰ接続を行う。

【００２６】ホスト１，２，３は、いずれも閉域網Ａのホストであることから、閉域網Ａを示すＶＬＡＮを利用する時に利用するＶＬＡＮを識別する情報、例えばＶＬＡＮタグとしてＶＬＡＮ１－ｘが割り当てられる。次に、同一閉域網からの複数のＰＰＰ回線を識別するために子番号ｘを割り当てる。ホスト１と３は、同一のＰＰＰ回線１から来ており、ＶＬＡＮタグとしてＶＬＡＮ１－１がＰＰＰ回線１と対応付けされている。また、ホスト２は、閉域網ＡのＰＰＰ回線２を利用して接続していることから、ＶＬＡＮタグとしてＶＬＡＮ１－２が該当するＰＰＰ回線２に対応付けされている。同様に、ホスト４，５は閉域網Ｂに属するホストであることから、閉域網Ｂを示すＶＬＡＮタグとしてＶＬＡＮ２－ｘが割り当てられることになる。閉域網Ａの場合と同様にＰＰＰ回線を識別するために、ホスト４にはＶＬＡＮ２－２がホスト５にはＶＬＡＮ２－１が割り当てられる。

【００２７】図１０に示すようにＶＮＡＴ機能を持つ装置ＶＮＡＴにおいてＶＬＡＮタグの割り当てに基づき閉域網から受け取ったパケットにこのＶＬＡＮタグを埋め込む。そして、このパケットは、ＩＥＥＥ８０２．１０やＶＬＡＮ対応のスイッチング機能などの既存のＶＬＡＮ技術によりServerまでこのＶＬＡＮタグに基づき運ばれる。パケットを受け取るServerは、図１１に示すようにＶＬＡＮタグ毎に別々の処理を行うために複数のＯＳが動作できるように変更し、閉域網を識別できる単位のＶＬＡＮタグに対し１つのＯＳが動作するようにする。つまり、ＶＬＡＮ１－ｘのタグに関する処理を行うためのＯＳ１，ＶＬＡＮ２－ｘのタグに関する処理を行うためのＯＳ２をという具合に１台のマシンの中で複数のＯＳを動作させることになる。サーバ側のネットワークにおいては、ＶＬＡＮタグを基にパケットの配送が行われるのでサーバ側のネットワーク上のサーバを含めて仮想的な閉域網を構築することができるので、パケットのアドレスに関してサーバ側では何ら変換を行う必要はない。このように、１台のサーバにおいてＶＬＡＮタグ毎にＯＳを動作させることでサーバ側の管理の下、閉域網の持つ閉域性を失うことなく仮想プライベートサーバを構築できる。

第２発明の変形

第２発明の変形例を以下に示す。ホスト１，２，３はいずれも閉域網Ａのホストであることから、閉域網Ａを示すＶＬＡＮタグとしてＶＬＡＮ１が割り当てられる。次に、同一閉域網からの複数のＰＰＰ回線が確立された場合に、パケットを受けとったＰＰＰ回線へとそのホスト宛のパケットを送り返すことができるように、ホストを示すアドレスとＰＰＰ回線を対応付ける。ホスト１と３は、同一のＰＰＰ回線１から来ており、各々のアドレスがＰＰＰ回線１へ対応付けられる。また、ホスト２は、閉域網ＡのＰＰＰ回線２を利用して接続していることから、ＶＬＡＮタグとしてはＶＬＡＮ１が割り当てられるが、ホスト２のアドレス２がＰＰＰ回線２に対応付けされる。

【００２８】同様に、ホスト４，５は閉域網Ｂに属するホストであることから、閉域網Ｂを示すＶＬＡＮタグとしてＶＬＡＮ２が割り当てられることになる。閉域網Ａの場合と同様に受けとったＰＰＰ回線にパケットを送り返すためにホストのアドレスとＰＰＰ回線とを対応付ける。この場合、ホスト４のアドレスがＰＰＰ回線２へ、ホスト５のアドレスがＰＰＰ回線１に対応付けられる。図１２に示すようにこのＰＰＰ回線とホストのアドレスの対応付けはＶＬＡＮタグ単位に行うので、ＶＬＡＮ１，ＶＬＡＮ２の各々独立して対応付けが行われる。参考までに、ＶＬＡＮ１に関する対応付けは以下のようなものとなる。この対応付けにおいて最新の接続時刻も合わせて管理して、タイムアウトを設けるなどによりセキュリティを高めることも出来る。サーバからのパケットを受けとるとこのＶＮＡＴ変換を行っている装置において、パケットに埋め込まれているＶＬＡＮタグをキーとして、まず検索する対応表を決め、次にパケットに埋め込まれているデスティネーションアドレス（ホストのアドレス）をキーとして対応表を検索し、送り出すべきＰＰＰ回線を調べる。その結果により、パケットを受けとったＰＰＰ回線へと送出することができる。

具体例

この発明の方法により可能となる仮想プライベートサーバを利用した具体例として、複数業者を対象とする調達業務の例を用いて述べる。今回、企業１が調達のために各々企業Ａ，Ｂに調達依頼をし、どちらか良い方を選択するために企業間でデータの登録、交換しあうことが必要となる場合での具体例である。

第１発明の具体例

図１３に示すようなネットワーク構成になっているとする。閉域網Ａ，Ｂ，１はそれぞれアクセスサーバＡＳ１，ＡＳ２，ＡＳ３によりインターネットと接続され、ＩＳＤＮ網がアクセスサーバＡＳ４によりインターネットと接続され、サーバ側ネットワークがルートサイドＮＡＴ機能付きアクセスサーバＲ－ＮＡＴによりインターネットと接続されている。また、ルートサイドＮＡＴ機能を持つ装置Ｒ－ＮＡＴにおいては図１４に示すようにアドレスの変換表を作成して動作する。変換表の作り方は後述する。ここで、閉域網Ｎは、企業Ｎの持つ閉域網を意味するものとする。サーバ網のネットワークにおか

れたルートサイドＮＡＴ機能付き装置Ｒ－ＮＡＴと各閉域網に置かれたアクセスサーバＡＳ１，ＡＳ２，ＡＳ３との間はトンネリングを利用してＰＰＰ接続される。また、ＩＳＤＮなどを利用してアクセスサーバＡＳ４に接続し、これを経由して閉域網に属するホストが直接サーバ側ネットワークにある装置Ｒ－ＮＡＴとＰＰＰ接続を行うこともできる。

【００２９】各閉域網のホストには所属する閉域網の持つアドレス空間から図１２に示すようにアドレスが各々割り振られている。このRoot-side ＮＡＴの機能を利用するために、サーバ側のネットワークにおいて各閉域網のためにアドレス空間をプールしてある。この例において、閉域網Ａにはエアアドレスで表わして１０．１０．１．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網Ａから接続してくる端末にアドレスを割り当てる。同様に、閉域網Ｂには１０．１０．２．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網Ｂから接続してくる端末に、閉域網１には１０．１０．１１．０サブネットマスク２５５．２５５．２５５．０のアドレス空間を用意し、この空間から閉域網１から接続してくる端末にアドレスを割り当てる。

【００３０】閉域網Ａにおいて、ホスト１は１０．０．１．１３、ホスト２は１０．０．３．２０、利用するWWW Server に１０．１．１．１が割り当てられているとする。実際には、WWW Server はサーバー側のネットワークにおかれていて、このWWW Server はサーバ一側のネットワークにおいて、１０．１００．１０．１が割り当てられ、異なる複数の閉域網に属する端末に対してサービスを提供している。サーバ側のネットワークにおいて閉域網Ａに割り当てられているアドレス空間１０．１０．１．０サブネットマスク２５５．２５５．２５５．０のうち、１０．１０．１．０サブネットマスク２５５．２５５．２５５．１９２はＰＰＰ回線１に、１０．１０．１．６４サブネットマスク２５５．２５５．２５５．１９２は、ＰＰＰ回線２に割り当てられている。そして、残りの空間１０．１０．１．１２８サブネットマスク２５５．２５５．２５５．１２８は動的にＰＰＰ回線１，２からの要求に応じてサブネットワーク単位で要求してきたＰＰＰ回線に割り当てるためにとってある。また、閉域網Ａの端末がWWW Server を利用する場合、サーバ側のネットワークにおいて、ポート番号８０８０番で閉域網Ａ用のサービスを展開するように設定されている。

【００３１】今、ホスト１がWWW Server を利用する場合、アクセスサーバ１（以下、ＡＳ１）から確立されるＰＰＰ回線１を利用するようになっている。もし、ＡＳ１とサーバ側のRoot-side ＮＡＴ機能付きＡＳ（以下、ＲＮＡＴ装置）との間にＰＰＰ回線１が確立していない場合、まずＰＰＰ接続を確立する。この時、ホストの認証だけでなくどの閉域網のどのＰＰＰ回線かを認証する。この場合、閉域網ＡのＰＰＰ回線１であることが認証される。次に、閉域網ＡのＰＰＰ回線１用にサーバ側ネットワークにおいて割り当てられているアドレス空間に利用していないアドレスがあるかをチェックする。今回の場合使用されていないアドレスがあるとし、その空間からホスト１に動的に１０．１０．１．１５が割り当てられる。もし、すでにＰＰＰ回線１用の空間がすべて使用されている場合、ＡＳ１がＰＰＰのＬＣＰなどを利用して必要な分のアドレス空間を要求し、これに応じてＲＮＡＴ装置において、閉域網Ａの持つ動的に割り当てるために用意されている空間１０．１０．１．１２８サブネットマスク２５５．２５５．２５５．１２８から要求のうち許可分を新たに複数のＰＰＰ回線１に割り当て、その中から動的にホスト１にアドレスを割り当てることになる。この時、割り当てる空間がどのＰＰＰ回線に割り当てたかをＲＮＡＴ装置で管理し、これによりパケットを適切なＰＰＰ回線へと送り出せる。動的に割り当てるのは、サブネット単位の要求分を割り当てる他に、決まった一定のサブネット空間分でもよいし、徐々にサブネット空間を単位として大きくしていってもよい。

【００３２】ホスト２は、閉域網Ａにおいてアドレスが１０．０．３．２０であり、ＡＳＩとＲＮＡＴ装置間に確立されるＰＰＰ回線２を利用してサーバに接続する。ホスト１が接続する場合と同様に、このＰＰＰ接続確立時にこのＰＰＰ回線が閉域網Ａに属するＰＰＰ回線２であることが認証される。そして、閉域網ＡのＰＰＰ回線２用に用意された空間１０．１０．１．６４サブネットマスク２５５．２５５．２５５．１９２から使用されていないアドレスを検索し、ホスト２に割り当てる。今回、ホスト２には、１０．１０．１．１００が動的に割り当てられる。もし、あらかじめ用意された空間がすべて使用されていたら、ホスト１の時と同様にして動的にアドレス空間をＰＰＰ回線２に割り当て、その空間から動的にホスト２に割り当てる。このようにして、接続してきたホストにサーバ側のネットワークにおいてアドレスが割り当てられ、ＲＮＡＴ機能に必要なアドレス変換表が作られる。

【００３３】ホスト１からWWW Server への場合、ＲＮＡＴ装置においてパケットのソースアドレスを１０．０．１．１３から１０．１０．１．１５へ、デスティネーションアドレスを１０．１．１．１から１０．１００．１０．１へと変換する。また、WWW Server を利用するために、サーバのポート番号８０にホスト１は利用要求を出すが、ＲＮＡＴ装置において閉域網Ａ用のサービスを提供しているサーバのポート番号８０８０にポート番号も変更して、変換後サーバ側ネットワークのルーティングにより正しくサーバに送られ、閉域網Ａ向けのサービスの利用が行われる。

【００３４】逆にWWW Server からホスト１へのパケットは、デスティネーションアドレスを１０．１０．１．１５から閉域網Ａに属するホスト１であることとＡＳ１から確立されているＰＰＰ回線１向けのパケットであることを識別し、アドレスを１０．０．１．１３へと変換する。次にホスト１が閉域網Ａに属しているという情報からソースアドレスを１０．１００．１０．１から１０．１．１．１へ変換する。そして、ポート番号も８０８０からホストが送ってきたパケットに指定されていたポート番号８０へと変換される。この変換後、受け取ったパケットの持つデスティネーションアドレスに基づく情報により適切なＰＰＰ回線である閉域網ＡのＰＰＰ回線１へパケットを送り出す。

【００３５】同様に、閉域網Ｂの場合について述べる。閉域網Ｂにおいて、ホスト３は１０．０．１．３０、ホスト４は１０．０．１．１４、利用するWWW Server に１０．１０．１５．１を割り当てているとする。実際には、WWW Server はサーバ側のネットワークにおかれていて、このWWW Server は前述同様、サーバ側のネットワークにおいて、１０．１００．１０．１が割り当てられている。サーバ側のネットワークにおいて、閉域網Ｂに割り当てられているアドレス空間は、１０．１０．２．０サブネットマスク２５５．２５５．２５５．０であり、閉域網Ｂでは、端末自身がＲＮＡＴ装置に直接ＰＰＰ接続する利用も行われており、そのために、１０．１０．２．６４．サブネットマスク２５５．２５５．２５５．１９２の空間をそれらのために用意し、各ＰＰＰ回線と１対１対応にアドレスを静的に割り振っている。今回、ＰＰＰ回線２以降が端末から直接確立されるＰＰＰ回線とし、ＰＰＰ回線２には、１０．１０．２．６５が割り当てられており、他の該当するＰＰＰ回線もアドレスが１つ静的に割り当てられている。また、ＡＳ２から確立されるＰＰＰ回線１用には１０．１０．２．０サブネットマスク２５５．２５５．２５５．１９２の空間を静的に割り当てており、このＰＰＰ回線を利用するホストにアドレスはこの空間から動的に割り当てられる。残りの空間１０．１０．２．１２８サブネットマスク２５５．２５５．２５５．１２８は割り当て分を使用したＰＰＰ回線１からの要求に応じて動的に割り当てるために用意してある。

【００３６】ホスト３はＡＳ２により確立されているＰＰＰ回線１を利用して接続しているので、閉域網Ａのホスト１や２の場合と同様に、利用しているＰＰＰ回線が閉域網ＢのＰＰＰ回線１であることが認証されると、静的に割り当てられた空間１０．１０．２．０サブネットマスク２５５．２５５．２５５．１９２に使用されていないアドレスがあるかを検索し、あればその中から任意なものを割り振る。今回、ホスト３にはサーバ側ネットワークにおいて、１０．１０．２．１０が割り当てられる。ホスト４は、今、移動しており最寄りのＡＳ４に着呼し、ＰＰＰトンネリングを利用してＲＮＡＴ装置に対して直接ＰＰＰ回線を確立する。この確立時に、ＰＰＰ回線が閉域網ＢのＰＰＰ回線２であることが認証され、ＰＰＰ回線２は静的にアドレスが１つ割り当てられており、この例では割り当てられているアドレス１０．１０．２．６５がホスト４のアドレスとなる。また、WWW Server のアドレスは閉域網Ａの場合と同じである。また、利用するサービスを示すポート番号は、閉域網Ｂにはポート番号８０８１が割り当てられている。

【００３７】実際のホストからWWW Server （ポート番号８０）への通信時には、ホスト１，２の場合と同様に図１４に示す変換表などによりＲＮＡＴ装置において、パケットの持つソースとデスティネーションアドレスを各々変換し、さらにポート番号に関して、８０から閉域網Ｂに対して指定されている８０８１番に変換される。逆にWWW Server からホストへのパケットも、前述と同様にパケットの持つソースとデスティネーション双方のアドレスとポート番号を変換する。この変換時に、パケットのデスティネーションアドレスによりホストの所属する閉域網がどれであるか、その閉域網から複数のＰＰＰ回線が存在する場合には、どのＰＰＰ回線へ送り出すかを判断できる。また、この情報を基にサーバに対して接続しているポート番号も変換される。そして、アドレスとポート番号が変換後、適切なＰＰＰ回線へと送出される。例えば、ホスト３へのパケットの場合は、１０．１０．２．１０がデスティネーションアドレスとして与えられているので、これにより閉域網ＢのＰＰＰ回線１へ送り出せば良いパケットであることが識別されて送り出される。

【００３８】閉域網１のホスト５の場合も同様に動作し、閉域網１の決めたアドレス空間の割り当て方針によりアドレスがホスト５に割り当てられ、図１３に示すような表が作られ、これを利用してアドレス変換がホスト５に関して行われる。また、閉域網１用に決められたサーバ利用時のポート番号８０８８とすると、ポート番号に関しても変換が行われる。サーバ側ネットワークからホストへのパケットに対しても前述と同様の仕組みにより適切な閉域網の適切なＰＰＰ回線へと送られる。

【００３９】ここで、アドレスは所属する閉域網を認証した結果としてサーバ側のネットワークにおいて割り振られるので閉域網を示すという意味においてアドレスは保証されていることになり、このアドレスを基に制限を行うことは、閉域網単位での制限を行うことと同等である。つまり、アドレス１０．１００．１０．１を持つWWW Server は、１０．１０．１．０サブネットマスク２５５．２５５．２５５．０、１０．１０．２．０サブネットマスク２５５．２５５．２５５．０、１０．１０．１１．０サブネットマスク２５５．２５５．２５５．０の各アドレス空間からの接続のみを許可することで、これ以外のアドレス、つまり他の閉域網からの利用

を容易に制限ができる。これにより、限られた閉域網間での通信を閉域性を保ちながらできる。また、アドレスを利用したデータへのアクセス制限だけでなく、今回のように閉域網単位で利用するポート番号を決めておき、そのポート番号単位にそれに応答するプログラムを動作させ、参照できるデータ、参照して変更できるデータなどを設定しておくことで物理的に一台のサーバによる複数閉域網向けにカスタマイズしたサービスが実現できる。

【００４０】今回の場合、閉域網Ａ，Ｂに割り当てているポート番号８０８０と８０８１に対して動作しているプログラムがアクセス、操作できるデータを各々区別することで、同一サーバ上にデータがあっても閉域網Ａは自分の登録したデータは参照・変更はできるが、閉域網Ｂの登録したデータは変更する事はもちろん見ることもできないようにできる。逆に、閉域網１に割り当てたポート番号８０８８に対して動作しているプログラムは、先のポート番号８０８０と８０８１で動作しているプログラムがそれぞれアクセス、操作できるデータの両方にアクセスすることが出来るようにすれば、閉域網１のホストは、閉域網Ａ，Ｂ双方が独立して管理するデータを参照できる。これにより、今回の例としている調達業務において要求される注文主の企業１が注文先である企業Ａ，Ｂ双方のデータを自由に見ることができるという課題がクリアされる。これは、今回のようにポート番号で制限を行ってもよいし、閉域網単位に割り当てたアドレス空間を用いて制限を行っても良い。また、異なるアドレス空間における通信を禁止することで、サーバ側のネットワークを介した異なる閉域網間での通信を防止でき、閉域網の持つ閉域性を維持することができる。さらには、接続先のサーバのアドレスもサーバ側で管理できるので、複数のサーバを用意しておけばサーバの負荷に応じてアドレスの変換を行うことでサーバの負荷分散も可能になる。

【００４１】次に、ＩＰネットワークによる通信時に重要な働きをするＤＮＳ（Domain Name System）サーバとの動きを、閉域網Ａとサーバ側ネットワークとの通信時を例として述べる。図１２において、まずユーザの閉域網に属するホストがサーバ側のネットワークのホストに接続する場合を述べる。閉域網Ａに属するホスト１がサーバ側ネットワークのWWWサーバに接続するために、閉域網Ａ上のＤＮＳサーバ２に接続したいWWWサーバのアドレスを問い合わせる。閉域網Ａのアドレス空間においてWWWサーバに対してアドレスが割り当てられているので、ＤＮＳサーバ２は閉域網Ａで該当するサーバに割り当てられたアドレス１０．１．１．１をホスト１に返す。そして、ホスト１は、ソースアドレスを自分の持つアドレス１０．０．１．１３、デスティネーションアドレスをサーバの持つアドレス１０．１．１．１、デスティネーションのポート番号８０としたパケットを送出する。そして、閉域網Ａのネットワークにおいて１０．１．１．１宛のパケットをＡＳ１へ届くように正しくルーティングを設定しておくことで、このパケットは、ＡＳ１に届き、必要ならばＰＰＰ回線を確立してサーバ側ネットワークのＲＮＡＴ機能付き装置まで運ばれる。このパケットを受け取ったＲＮＡＴ機能付き装置はパケットのデスティネーションアドレスを自身の持つ変換表を基に、１０．１．１．１から１０．１００．１０．１へと変換する。次に、ソースアドレスの１０．０．１．１３を変換表の中において検索する。検索した結果、該当するアドレスが存在するとそのアドレスを利用して、今回の例の場合は１０．１０．１．１５に変換し、さらにデスティネーションのポート番号８０を、閉域網Ａ用に割り当てられたポート番号８０８０に変換され、そのパケットは該当するサーバへと運ばれる。もし、該当するアドレスがない場合は前述の方法によりサーバ側ネットワークにおいて割り当てられ、以下通常の場合と同様に通信が行われる。

【００４２】もし、仮にＤＮＳサーバ２に接続したいサーバのアドレスが登録されていない場合、ＤＮＳサーバ２はサーバ側ネットワークのＤＮＳサーバであるＤＮＳサーバ１にサーバのアドレスを問い合わせる。この問い合わせパケットはルーティングによりＡＳ１を経由してサーバ側ネットワークのＲＮＡＴ装置に送られる。受け取ったＲＮＡＴ装置は、パケットのソースとデスティネーションアドレスの両方を変換表に基づき変換する。そして、該当パケットがＤＮＳのアドレス問い合わせパケットの場合、パケットのデータには変更を加えずＤＮＳサーバ１へ送る。ＤＮＳサーバ１は、指定された接続先のサーバのアドレスをレスポンスとして返す。今回の場合、サーバのアドレス１０．１００．１０．１がデータとして埋め込まれる。このレスポンスパケットは、サーバ側ネットワークのルーティングによりＲＮＡＴ装置へと送られる。受け取ったＲＮＡＴ装置はデスティネーションアドレス１０．１０．１．６２（サーバ側ネットワークにおいて閉域網ＡのＤＮＳサーバ１に静的に割り当てたアドレス）からパケットが閉域網ＡのＡＳ１から来ているＰＰＰ回線１に送り出せばよいことを識別し、閉域網Ａに関する変換により正しくソースとデスティネーションアドレスを変換する。また、このパケットがＤＮＳのレスポンスパケットでありホストのアドレスを返すものである場合、データとして埋め込まれたサーバのアドレス１０．１００．１０．１を閉域網Ａにおいて割り当てられたサーバのアドレスである１０．１．１．１．に変換され、このパケットはＤＮＳサーバ２へと送られる。これを受け取ったＤＮＳサーバ２は、１０．１．１．１を接続したいサーバのアドレスとしてホスト１へ答え、ホスト１は通常の接続と同様にパケットを送出し通信を行う。

【００４３】逆にサーバ側ネットワーク上のWWWサー

バが閉域網のホスト１に接続する場合について述べる。まず、サーバ側ネットワークのサーバがホスト１のアドレスをＤＮＳサーバ１に問い合わせる。ＤＮＳサーバ１はホスト１のアドレスを知らないので、ホスト１の名前に含まれているドメイン名などからホスト１がまず閉域網Ａに属するホストであることを認識する。そして、閉域網ＡのＤＮＳサーバであるＤＮＳサーバ２に対してサーバ側ネットワークで割り当てたアドレス（今回の場合、１０．１０．１．６２）をデスティネーションアドレスとしてアドレス問い合わせのパケットを送出する。このパケットはサーバ側のネットワークにおいてＲＮＡＴ装置へとルーティングされる。パケットを受け取ったＲＮＡＴ装置はデスティネーションアドレスから閉域網ＡのＰＰＰ回線１向けのパケットであることを識別し、閉域網Ａのアドレス空間へとソースとデスティネーションアドレスの両方を自身の持つ変換表により変換する。そして、閉域網ＡのＤＮＳサーバ２へと送出される。

【００４４】このパケットを受け取ったＤＮＳサーバ２は、問い合わせられているホスト１の閉域網Ａでのアドレス１０．０．１．１３をレスポンスとして、サーバ側ネットワークのＤＮＳサーバ１へと送る。このパケットはサーバ側ネットワークのＲＮＡＴ装置が受け取り、まずソースとデスティネーションアドレスを各々変換表より変換する。そして、このパケットがホストのアドレス問い合わせの答えであることからデータに埋め込まれているホストのアドレス部分をサーバ側ネットワークのアドレスへと変換する。この時、ＲＮＡＴ装置の持つ変換表を検索し該当するデータがあれば、変換表から対応するアドレスへと変換して、ＤＮＳサーバ１へ送る。また、該当するデータがない場合は、前述の方法によりホスト１へ閉域網ＡのＰＰＰ回線１用に割り当てたアドレス空間から動的にアドレスを割り当て、割り当てたアドレスへＤＮＳサーバ２からのレスポンスであるホスト１のアドレスを変更し、ＤＮＳサーバ１へ送る。今回は、アドレス１０．１０．１．１５が割り当てられ変換されることになる。この時、ＲＮＡＴ装置の持つ変換表に該当するホスト１に関するアドレスデータを付加する。このようにＤＮＳサーバのレスポンスであるホストのアドレスは変換され、変換されたアドレスが該当する閉域網のホストに接続要求しているサーバへと通知される。そして、通知されたアドレスをデスティネーションアドレスとして、サーバは閉域網に属するホストへの接続を試み、ＲＮＡＴによるアドレス変換機能によりサーバ側からホストへの接続が確立されて通信が開始される。

【００４５】このようにすることでＤＮＳサーバとの連携が可能であり、既存のＤＮＳサーバに変更を加える必要がなく利用が可能となり、多くの通信に利用されているＩＰネットワークでの導入が容易であり、またサーバと閉域網のホストの双方向からの接続の確立が実現できる。また、ＤＮＳサーバを利用してアドレスの通知を制限すればサーバからの接続ができる閉域網のホストを限定するなど細かな制御も出来、閉域網の方針による閉域性の維持ができる。

【００４６】以上から、サーバ側のネットワークにおいて各閉域網毎にアドレス空間を用意し、さらには、各閉域網ごとにサーバに対して利用できるポート番号を決めて、受けとった／送り出すパケットの該当する各部分を変換しているので、サーバ側から端末への情報配信や閉域網毎、あるいは、地域毎にカスタマイズしたサービスの実現が可能になる。さらに閉域網単位にアドレスを割り当てるので閉域網の持つ閉域性を保持したまま複数閉域網に対し１台のサーバによるサービスの提供ができる仮想プライベートサーバの構築を可能にする。また、動的に割り当てるアドレスの割り当て有効期限をある一定時間／あるイベント終了までとすることで、一度動的に割り当てたアドレスの再利用が可能でありスケーラビリティやセキュリティを確保することも可能である。

第２発明の具体例

第１発明の具体例の場合と同様に、企業１が企業Ａ，Ｂに対して調達を行う場合を例にして述べる。ネットワークの構成は、図１５に示すようなものとなっている。即ち閉域網Ａ，Ｂ，１はそれぞれアクセスサーバＡＳ１，ＡＳ２，ＡＳ３によりインターネットと接続されサーバ側ネットワークはＶＮＡＴ機能付きアクセスサーバによりインターネットと接続されている。閉域網Ｎは、企業Ｎの持つ閉域網を示している。また、ＶＮＡＴ機能を持つ装置においては図１６に基づき各閉域網のＰＰＰ回線単位にＶＬＡＮタグを割り当てる。ホスト１がサーバ側ネットワーク上のサーバを利用する時、ＡＳ１とＶＮＡＴ機能付ＡＳ（以下、ＶＮＡＴ装置）との間にＰＰＰ接続がなければＰＰＰ接続を確立する。このＰＰＰ接続確立時の認証において、このＰＰＰ回線が閉域網ＡのＰＰＰ回線１であることが認証される。閉域網Ａを示すＶＮＡＴタグとしてＶＬＡＮ１が割り当てられており、これまでＰＰＰ回線１を示すために子番号を用いてこのＰＰＰ回線１に対してＶＮＡＴ１－１というＶＬＡＮタグが割り当てられる。これにより、閉域網ＡのＰＰＰ回線１であることを識別できる。ＰＰＰ回線２が確立した場合は、ＶＬＡＮ１－２というように子番号をＰＰＰ回線に対応させるものとする。ＶＬＡＮタグの形式は既存のＶＬＡＮ技術を利用するために、ＩＥＥＥ８０２．１０などで定義されているものなど既存のものを用い、情報量としてここに述べたどの閉域網のどのＰＰＰ回線であるか識別できるものであればよい。

【００４７】ＶＮＡＴ機能によりこのＰＰＰ回線を通してサーバ側のネットワークに来るパケットに関しては、図９に示したようにＶＬＡＮタグを埋め込み、このタグを基にサーバへ配送される。そして、サーバではＶＬＡＮタグ毎に様々な処理を行うプログラム、例えばＯＳを別個に動作させ処理を行う。このサーバではＶＬＡＮタ

グと接続してきたホストの情報を関連付けることでホストへ向けてパケットの送出時には、適切なＶＬＡＮタグをつけて送り出すことができる。これにより、サーバ側ネットワークでのアドレスの変換は必要とすることなく、自閉域網に存在するかのようにサーバを利用できる。また、ＶＬＡＮタグ毎にＯＳが動作しているためにその動作は閉域網単位で柔軟に変更できるようになっており、参照・登録するデータもＶＬＡＮタグをキーにして制限をかけることができる。サーバ側ネットワークから閉域網へ送り出される時には、受け取ったパケットについているＶＬＡＮタグを取り除き、ＶＬＡＮタグからパケットの配送先として適切な閉域網と適切なＰＰＰ回線を識別し正しいＰＰＰ回線へと送り出す。

【００４８】ホスト２がサーバ側のネットワークに接続する場合は、ＰＰＰ回線２を利用するので、このホスト２からサーバ側ネットワークへのパケットには前述の方法と同様にＶＬＡＮタグが割り当てられＶＬＡＮ１－２を用いることになる。このタグを用いて、ホスト１の場合と同様に動作する。各々のパケットに埋め込まれるＶＬＡＮタグは異なるが、サーバは閉域網Ａを示すＶＬＡＮ１を基にして動作を決定するので、利用するＰＰＰ回線が異なっていても同一のデータを参照・変更できる。逆に、サーバからホスト１，２へのパケットはＶＬＡＮタグにより閉域網Ａへのものであることが識別され、さらにＶＬＡＮタグの子番号を基にホスト１へのパケットはＰＰＰ回線１へ、ホスト２へのパケットはＰＰＰ回線２へと適切に振り分けられる。

【００４９】ホスト３，４は同じＡＳ２を介してサーバ側ネットワークに接続しており、ともにＰＰＰ回線１を利用しているので、利用するＶＬＡＮタグは同じでＶＬＡＮ２－１を用いて、ＶＮＡＴ装置においてパケットに組み込まれ、サーバへと送られる。サーバからホストへのパケットも前述のホスト１と同様にして適切なＰＰＰ回線を通りホストへと送られる。

【００５０】ホスト５の場合も同様に、ＰＰＰ接続確立時に所属する閉域網が閉域網１であり、これがＰＰＰ回線１であることが認証され、それに基づき閉域網１を示すＶＬＡＮタグであるＶＬＡＮ３、ＰＰＰ回線１を示すＶＬＡＮタグであるＶＬＡＮ３－１が割り当てられる。そして、他のホスト同様の動作により正しくホストとサーバ間においてやり取りされる。また、ＶＬＡＮタグがＶＬＡＮ３に関する処理をするＯＳからは、ＶＬＡＮタグがＶＬＡＮ１，ＶＬＡＮ２しか参照できないデータを参照することが出来るようにすることで、企業１のユーザは、企業Ａ，Ｂが登録したデータを見ることができ、今回の例となっている調達業務に必要となる制限付きの閉域網間の通信が実現される。

【００５１】次に、ＩＰネットワークによる通信時に重要な動きをするＤＮＳ（Domain Name System）サーバとの動きであるが、第２発明の場合はサーバは確かにサーバ側のネットワーク上にあるが、ＶＬＡＮ機能の利用により仮想的に閉域網内での通信が実現されているので、ＤＮＳサーバは通常の場合と同様の利用が可能であり、サーバに割り当てられたアドレス宛のパケットが正しく閉域網においてサーバ側のネットワークにあるＶＮＡＴ装置とＰＰＰ接続できるＡＳへと正しくルーティングされるように設定するだけで利用が可能になる。

【００５２】このようにして、サーバのアドレスをデスティネーションアドレスとし、そのパケットがサーバ側ネットワークへ運ばれるようにするなど、ユーザ側のネットワークに変更を最小限にしてサーバ側の制御のもと１台のサーバにより複数の閉域網に対して各々サーバがあるかのように動作できる仮想プライベートサーバによるサービスの提供が可能になる。

【００５３】第２発明の変形に対する具体例を以下に示す。ＰＰＰ回線確立時に所属する閉域網の認証を行い、閉域網単位で、ＰＰＰ回線と受けとったパケットの送出元であるホストのアドレスとを対応付ける。今回の場合、図１７に示すような表をＶＮＡＴ装置が持つことになる。また各閉域網Ａ，Ｂ…に対してＶＬＡＮタグ，ＶＬＡＮ１，ＶＬＡＮ２，…が予め割り当てられてある。

【００５４】ホスト１がサーバ側ネットワークに接続を試みると、ＡＳ１とＶＮＡＴ装置との間にＰＰＰ回線１が確立され、閉域網Ａであることが認証される。そして、この認証結果によりＶＬＡＮタグのＶＬＡＮ１がこのＰＰＰ回線１に割り当てられる。そして、ホスト１からのパケットがＶＮＡＴ装置に到着すると、ＶＮＡＴ装置ではパケットに埋め込まれたホスト１のアドレス１０．０．１．１３と、パケットが運ばれてきたＰＰＰ回線１とを対応付ける。そして、認証結果により割り当てられたＶＬＡＮタグを埋め込み、サーバへと送られる。逆に、サーバからパケットが到着すると、埋め込まれたＶＬＡＮタグのＶＬＡＮ１により図１７の対応表からＶＬＡＮ１に関するものを選択し、パケットのデスティネーションアドレスであるホスト１のアドレス１０．０．１．１３をキーにして検索を行い、対応表よりこのパケットを閉域網Ａとの間に確立されたＰＰＰ回線１に送り出せばよいことを認識し、ＶＬＡＮタグを取り除きＰＰＰ回線１へと送り出す。このようにして、同一の閉域網から複数のＰＰＰ回線が確立された場合でも、パケットを受けとったＰＰＰ回線へ正しくパケットを送り出すことができる。

【００５５】ホスト２の場合は、閉域網Ａに属するホストであるので、ホスト１と同様にＶＬＡＮ１が割り当てられる。しかし、利用しているＰＰＰ回線がホスト１と異なるので、ホスト２のアドレス１０．０．３．２０はＰＰＰ回線２へと対応付けされる。これにより、ホスト１と同様にＶＬＡＮ１がパケットに埋め込まれるが、サーバからのパケットはこの対応表により、ホスト２宛のパケットは適切にＰＰＰ回線２を利用して送られる。ホ

25

ストラ，４，５の場合も同様の方法によりＶＬＡＮタグが割り当てられ、ホストのアドレスとＰＰＰ回線が割り当てられ、ＶＬＡＮタグ単位で独立して管理される。これにより、適切な閉域網の適切なＰＰＰ回線へとパケットを送り出すことができる。

【００５６】次に図１８を参照して図１中のＲ－ＮＡＴ装置、つまりルートサイドＮＡＴ機能付きアクセスサーバの概略機能構成を説明する。複数のＰＰＰ回線処理部１１が設けられＰＰＰ回線処理部１１には認証部１２が付属されている。ＰＰＰ回線確立の際にどの閉域網のどのＰＰＰ回線であるかの認証が認証部１２で確認され、図２Ｂに示したアドレス割り当てテーブル１３を参照してそのＰＰＰ回線を利用して到着したパケットのホストにサーバ側ネットワークの割り当て分のうち空きアドレスが割り当てられ、その各閉域網のＰＰＰ回線と閉域網側のアドレスと、割り当てたサーバ側ネットワークのアドレスとの対応表（変換表）１４が作られる。ＰＰＰ回線処理部１１に端末からパケットが来ると、そのＰＰＰ回線が確立していれば、その閉域網とＰＰＰ回線に該当する対応表１４を参照して、そのパケットのアドレスに対して、アドレス変換部１５でアドレス変換を行ってサーバ側ネットワークへ送られる。サーバ側ネットワークからのパケットは、そのアドレスにより対応表１４を参照して、閉域網側で付与したアドレスに変換すると共にどの閉域網のどのＰＰＰ回線かを知り、対応するＰＰＰ回線処理部１１よりＰＰＰ回線へ送出する。

【００５７】このＲ－ＮＡＴ装置において閉域網からパケットに対する処理は図１９に示すようになる。まず最初のパケットの到来に先立ち、ＰＰＰ回線接続要求があるかがＰＰＰ回線処理部１１で調べられ（Ｓ１）、接続要求であればどの閉域網のどのＰＰＰ回線からの要求であるかを認証し（Ｓ２）、ＰＰＰ回線を確立する（Ｓ３）。

【００５８】この状態でそのＰＰＰ回線を利用したホストからのパケットを待ち（Ｓ４）、パケットが到来すると、その閉域網とソースアドレスにより対応表１４を検索し（Ｓ５）、対応するものがなければ、そのパケットのアドレスに対し、アドレス割り当てテーブル１３を参照してサーバ側ネットワークのアドレスを割り当て、これらの関係を対応表１４に書込む（Ｓ６）。到来パケットについてそのアドレスで対応表１４を検索し、アドレス変換部１５でアドレス変換してサーバ側ネットワークへ送る（Ｓ７）。その後に到来するパケットはＰＰＰ回線が確立されているから、ステップＳ４のパケット待ち状態にあり、また対応表１４の検索によりアドレスが見つかる場合は（Ｓ５）、対応表（変換表）１４にもとづくアドレス変換を行ってサーバ側ネットワークへ送出する（Ｓ７）。見つからない場合は、上記のようにアドレス割り当て対応表１４を作成する。

【００５９】次に図８中のＶＮＡＴ装置（ＶＮＡＴ機能

26

付きアクセスサーバ）の概略機能構成を図２０を参照して説明する。図１８の場合と同様に複数のＰＰＰ回線確立部１１、これに付属する認証部１２が設けられ、ＰＰＰ回線確立時に、どの閉域網のどのＰＰＰ回線かが認識され、そのＰＰＰ回線には図９に示すようなＶＬＡＮタグテーブル２１によりその閉域網のそのＰＰＰ回線と対応したＶＬＡＮタグが割り当てられる。そのＰＰＰ回線を通じて到来したパケットに対し、パケット変換部２２で、そのＰＰＰ回線に割り当てられたＶＬＡＮタグが付加されて、サーバ側ネットワークへ送出される。

【００６０】サーバ側ネットワークから到来したパケットは、パケット変換部２２でそのＶＬＡＮタグによりＶＬＡＮタグテーブル２１を検索し、対応するＰＰＰ回線へ、ＶＬＡＮタグを除去して送出する。このＶＮＡＴ装置における閉域網からのパケットに対する処理は図２１に示すようになる。まず最初のパケットの到来に先立ち、ＰＰＰ回線接続要求があり（Ｓ１）、どの閉域網のどのＰＰＰ回線からの要求であるかの認証を行い（Ｓ２）、ＰＰＰ回線を確立する（Ｓ３）。

【００６１】その後、その確立したＰＰＰ回線にパケットが到来すると（Ｓ４）、その閉域網のそのＰＰＰ回線でＶＬＡＮタグテーブル２１を検索して該当するＶＬＡＮタグを取出し（Ｓ５）、これをパケット変換部２２でパケットに埋込みサーバ側ネットワークへ送る（Ｓ６）。ＶＬＡＮタグとして、ＰＰＰ回線を区別する番号を用いない、図１２や図１７を参照して説明した場合においてはＶＮＡＴ装置は図２０中のＶＬＡＮタグテーブル２１が閉域網とＶＬＡＮタグとの対応を示すものとなり、更に図２０中に破線で示すようにＰＰＰ回線が確立され、埋込むＶＬＡＮタグが決まると、図１２又は図１７に示すような、そのＶＬＡＮタグとそのＰＰＰ回線と、そのパケットの閉域網の（ソース）アドレスとの関係を示す対応表２３を作成する。サーバ側ネットワークからのパケットは、そのＶＬＡＮタグと、その（デスティネーション）アドレスとにより対応表２３を参照してパケット変換部２２でどの閉域網のどのＰＰＰ回線へ、ＶＬＡＮタグを除去したパケットを送るかを決定する。

【００６２】図２１に示した処理においては、ステップＳ６の代りに破線で示すようにＶＬＡＮタグを埋込み送出すると共にＶＬＡＮタグと、到来したＰＰＰ回線と（ソース）アドレスとの対応表を作成することになり、その他は同様である。上述では複数閉域網間の通信にこの発明を適用したが、複数ユーザ側ネットワークとサーバ側ネットワークとの通信にもこの発明は適用できる。

【００６３】

【発明の効果】この発明では、ＰＰＰ接続により各閉域網がサーバ側のネットワークに接続され、このＰＰＰ接続確立時に所属する閉域網とＰＰＰ回線自体を認証することにより、閉域網単位に割り当てたアドレス空間により様々な制御がサーバ側で容易に行える。これにより、

27

複数の閉域網のユーザ端末に対し、閉域性を失うことなく各閉域網にカスタマイズした共通サービスの提供を物理的に１台のサーバにより可能にし、各閉域網からは自閉域網に各々サーバが存在するように利用できる。また、今後増えゆくと予想される複数企業間でのデータ交換を必要とするプロジェクトの実施時や調達業務の実施時に必要となる複数閉域網向けの共用サーバの構築、運用などを提供するハウジングサービスが展開できる。このサービスを利用することで、ユーザは自社の閉域網を変更せず、また、閉域性を失う事なく容易にプロジェクト毎に一時的に必要となる共用サーバの運用ができ、複数の企業と連携して行うプロジェクトの情報化がスムーズに行えるので、この発明により実現されるサービスは、現在ＩＳＰ（Internet Service Provider）が行っているＶＰＮ（Virtual Private Network)サービスの新しい付加サービスとしての展開が見込める。また、この方法により実現されるサーバ側から閉域網のホストへの閉域性を維持しての接続確立が可能であることを利用して、サーバ側ネットワークに複数の閉域網で提供されている種々のサービスを統合的に利用できるサーバを構築し、個人向けのポータルサイトサービスの展開も可能になる。このように、この発明は閉域網向けの新しい情報流通プラットフォームを構築する手段としての利用が見込める。

【図面の簡単な説明】

【図１】第１発明を適用したシステムの構成例を示す図。

【図２】Ａは図１中のＲ－ＮＡＴにおけるアドレス変換テーブルの例を示す図、Ｂは各閉域網に対する、サーバ側ネットワークのアドレス空間の割り当て例を示す図である。

【図３】ホスト１についてのパケットの変換の様子を示す図。

【図４】ネットワークアドレス変換のイメージを示す図。

28

【図５】閉域網に割り当てられたネットワークアドレス空間の利用方針を示す図。

【図６】パケットにおけるアドレス変換の様子を示す図。

【図７】第１発明と従来技術との特徴の関係を示す図。

【図８】第２発明を適用したシステムの構成例を示す図。

【図９】ＶＬＡＮタグの割り当て例を示す図。

【図１０】ＶＮＡＴ機能のパケットに対する動作を示す図。

【図１１】ＶＮＡＴタグを利用したサーバ内の動作を示す図。

【図１２】第２発明におけるＶＬＡＮタグの対応付けの例を示す図。

【図１３】第１発明の具体例におけるシステムを示す図。

【図１４】図１２中のＲ－ＮＡＴ装置でのアドレス割り当ての例を示す図。

【図１５】第２発明の具体例におけるシステムを示す図。

【図１６】図１５中のＶＮＡＴ装置におけるＶＬＡＮタグの割り当て例を示す図。

【図１７】第２発明の変形におけるＶＬＡＮタグとアドレスとＰＰＰ回線の対応を示す図。

【図１８】Ｒ－ＮＡＴ装置の概略機能構成を示す図。

【図１９】Ｒ－ＮＡＴ装置における処理の一部を示す流れ図。

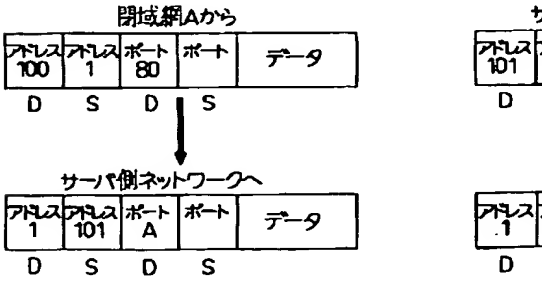
【図２０】Ｖ－ＮＡＴ装置の概略機能構成を示す図。

【図２１】Ｖ－ＮＡＴ装置における処理の一部を示す流れ図。

【図２２】従来のＰＰＰトンネリング接続のシステムを示す図。

【図２３】従来のＮＡＴによる接続のシステムを示す図。

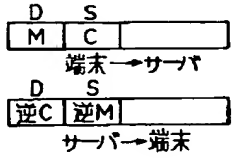
【図３】



S:ソース
D:デスティネーション

図3

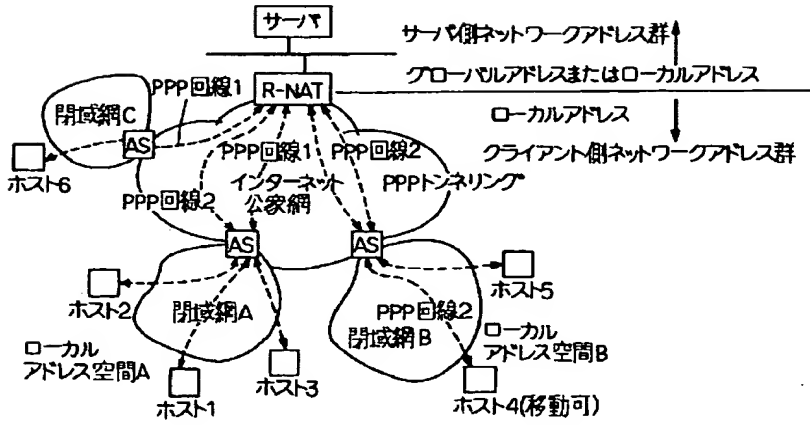
【図６】



S:ソース
D:デスティネーション
C:Compaction変換
M:Merge変換

図6

【図1】



R-NAT：Root-side NAT機能付きアクセスサーバ
AS：アクセスサーバ

図1

【図11】

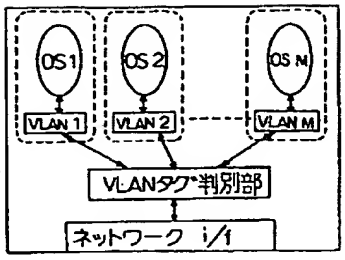


図11

【図2】

A

	閉域網 A	閉域網 B	サーバ側ネットワーク
ホスト1	アドレス1	—	アドレス101
ホスト2	アドレス2	—	アドレス220
ホスト3	アドレス3	—	アドレス102
ホスト4	—	アドレス11	アドレス301（静的）
ホスト5	—	アドレス22	アドレス321
Server	アドレス100	アドレス150	アドレス1

B

	閉域網 A	閉域網 B
割り当て空間	アドレス空間101-300	アドレス空間301-350
PPP回線1	アドレス空間101-200	アドレス空間311-350
PPP回線2	アドレス空間201-250	アドレス301
動的割り当て	アドレス空間251-300	—

図2

【図5】

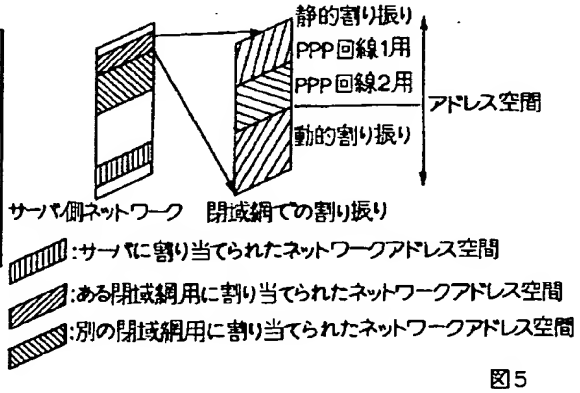


図5

【図7】

	従来のNAT	PPP トンネリング	方法1 (Root-side NAT)
ローカルアドレスの使用	○	○	○
サーバープッシュ型情報配信	×	×	○
カスタマイズドサービスの提供	△	×	○
不正アクセスパスの発生防止	×	×	○

図7

【図16】

	閉域網 A	閉域網 B	閉域網 1
PPP回線1	VLAN 1-1	VLAN 2-1	VLAN 3-1
PPP回線2	VLAN 1-2	—	—

図16

【図4】

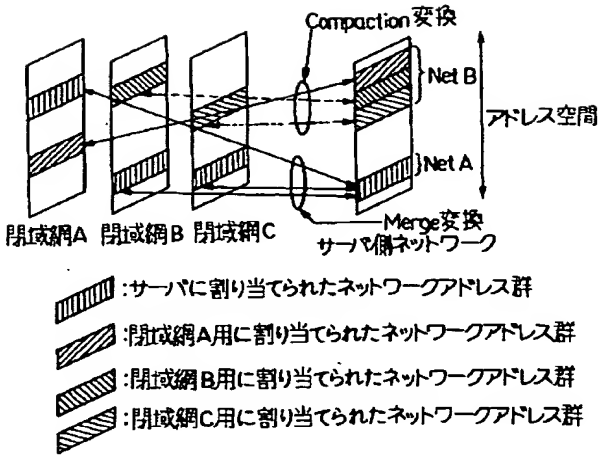
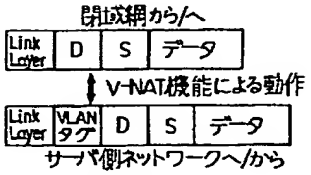


図4

【図10】



S:ソースネットワークアドレス
D:デスティネーションネットワークアドレス

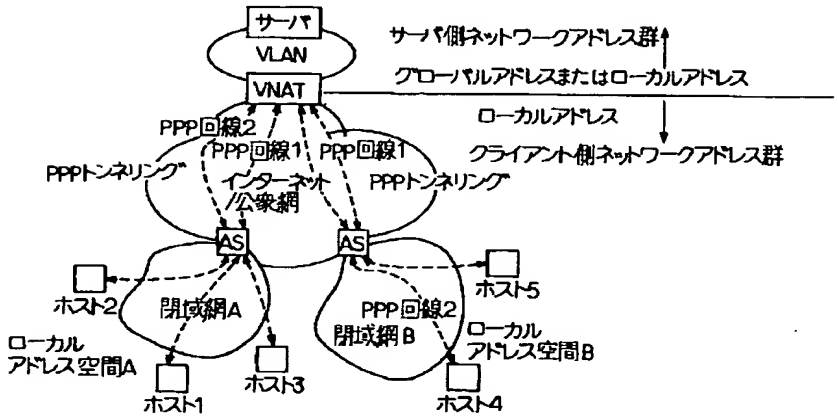
図10

【図17】

VLANタグ	アドレス	PPP回線番号
VLAN 1	10.0.1.13	PPP回線1
VLAN 1	10.0.3.20	PPP回線2
VLAN 2	10.0.1.30	PPP回線1
VLAN 2	10.0.1.14	PPP回線1
VLAN 3	10.1.1.1	PPP回線1

図17

【図8】



VNAT:VNAT機能付きアクセスサーバ
AS:アクセスサーバ

図8

【図9】

	閉域網 A	閉域網 B	VLANタグ
ホスト1	アドレス1	—	VLAN 1-1
ホスト2	アドレス2	—	VLAN 1-2
ホスト3	アドレス3	—	VLAN 1-1
ホスト4	—	アドレス11	VLAN 2-2
ホスト5	—	アドレス22	VLAN 2-1
Server	アドレス100	アドレス150	アドレス1

図9

【図12】

VLANタグ	ホストのアドレス	PPP回線番号
VLAN1	アドレス1	PPP回線1
VLAN1	アドレス2	PPP回線2
VLAN1	アドレス3	PPP回線1
VLANタグ	ホストのアドレス	PPP回線番号
VLAN2	アドレス4	PPP回線2
VLAN2	アドレス5	PPP回線1

図12

【図１３】

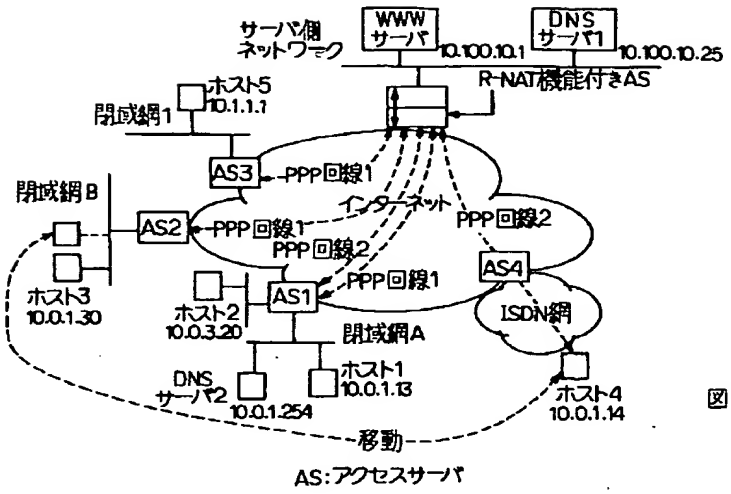


図13

【図１４】

	閉域網 A	閉域網 B	閉域網 1	サーバ側ネットワーク
ホスト１	10. 0. 1. 13	—	—	10. 10. 1. 15
ホスト２	10. 0. 3. 20	—	—	10. 10. 1. 100
ホスト３	—	10. 0. 1. 30	—	10. 10. 2. 10
ホスト４	—	10. 0. 1. 14	—	10. 10. 2. 65
ホスト５	—	—	10. 1. 1. 1	10. 10. 11. 1
Server	10. 1. 1. 1	10. 10. 15. 1	10. 50. 1. 1	10. 100. 10. 1

図１４

【図２２】

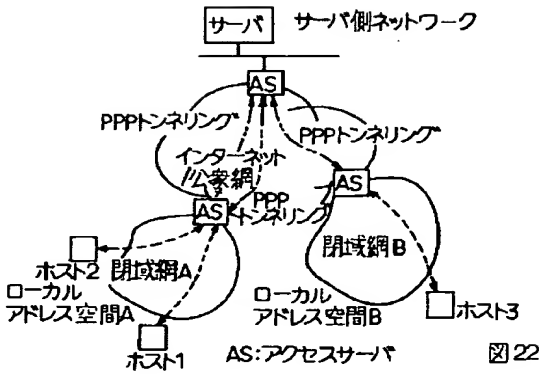


図22

【図１５】

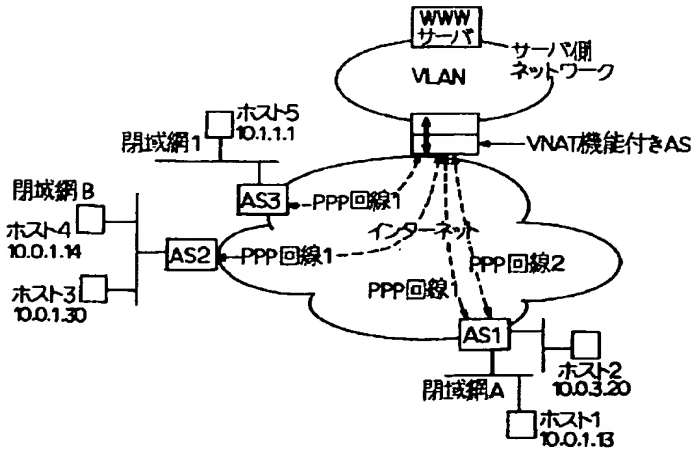


図15

【図18】

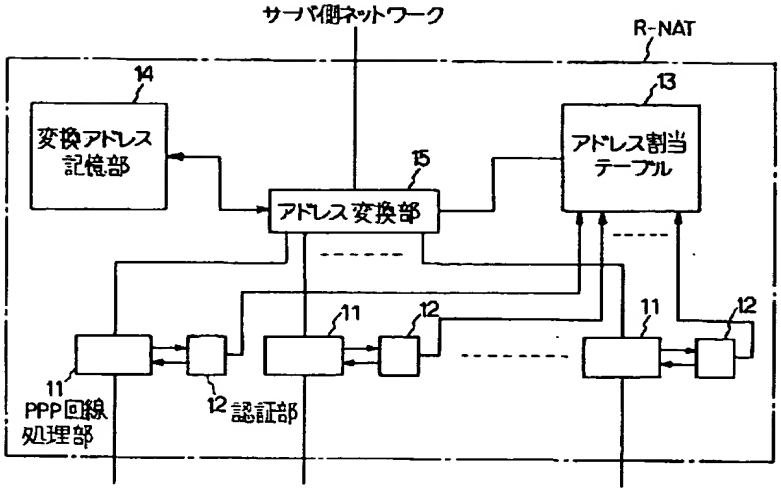


図18

【図19】

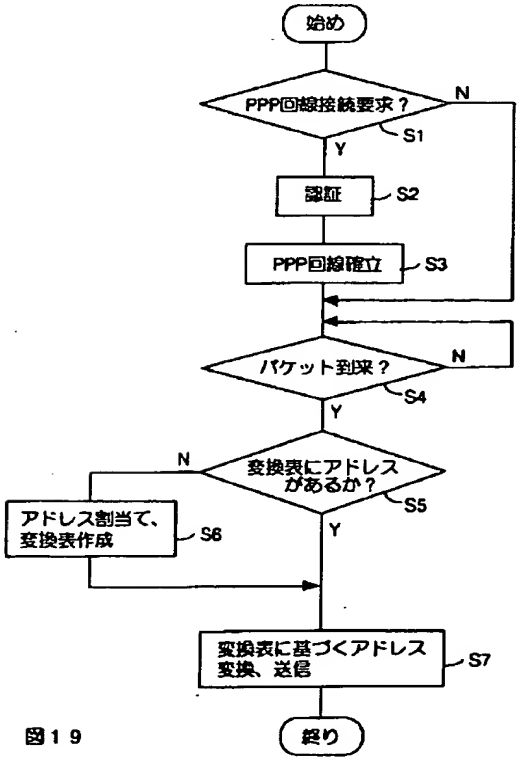


図19

【図21】

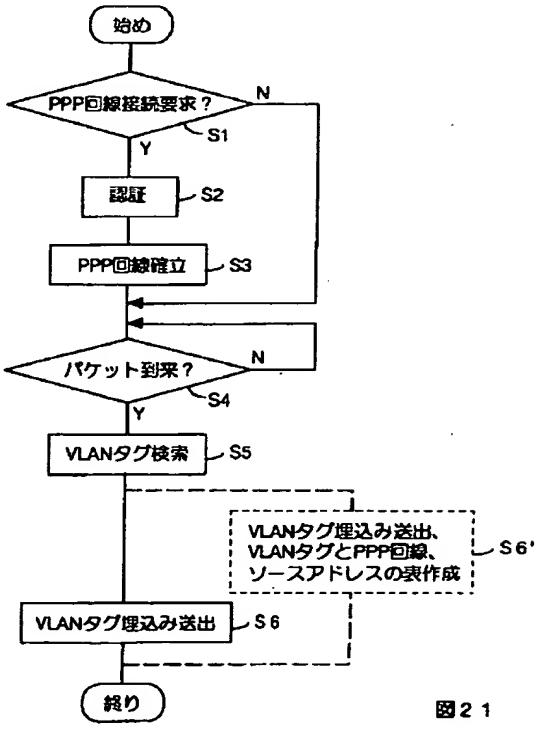


図21

【図２０】

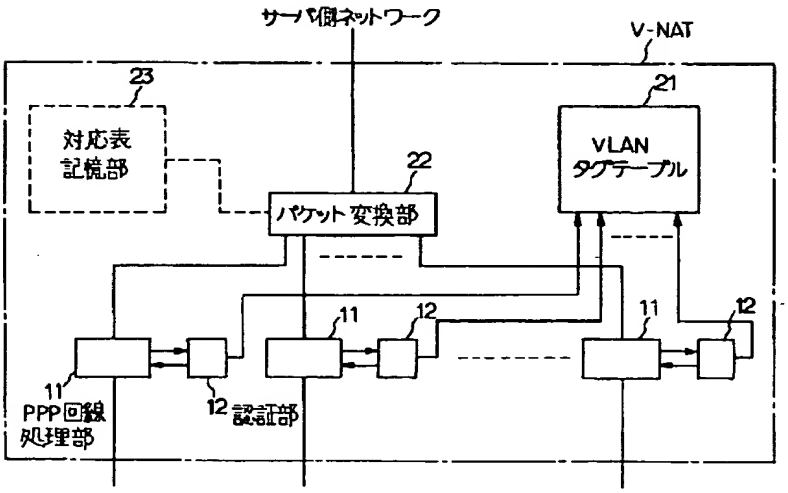


図20

【図２３】

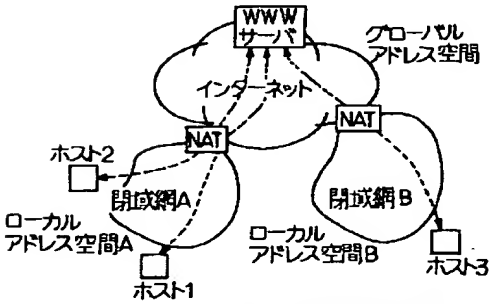


図23